WILLKIE FARR & GALLAGHER LLP
BENEDICT Y. HUR (SBN: 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN: 246943)
sagnolucci@willkie.com
EDUARDO E. SANTACANA (SBN: 281668)
esantacana@willkie.com
NOORJAHAN RAHMAN (SBN: 330572)
nrahman@willkie.com
ARGEMIRA FLÓREZ (SBN: 331153)
aflorez@willkie.com
HARRIS MATEEN (SBN: 335593)
hmateen@willkie.com
One Front Street, 34th Floor
San Francisco, CA 94111
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, et al. individually and on behalf of all others similarly situated,

Plaintiff,

vs.

GOOGLE LLC, *et al*.,

Defendant.

Case No. 3:20-CV-04688 RS

GOOGLE LLC'S OPPOSITION TO PLAINTIFFS' MOTION FOR CLASS CERTIFICATION AND APPOINTMENT OF CLASS REPRESENTATIVES AND CLASS COUNSEL

Date: **October 5, 2023**
Time: **1:30 p.m.**
Judge: **Hon. Richard Seeborg**
Ctrm. 3, 17th Floor, SF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

Google provides analytics services to millions of apps through a product called Google Analytics for Firebase ("GA4F"). When they filed this case, Plaintiffs alleged that Google had engaged in a massive campaign to deceive users by falsely telling them it would not target them with personalized advertising when using apps supported by GA4F, if a certain Google account setting called "supplemental Web & App Activity" ("sWAA") was turned off. Compl., Dkt. 1 (Jul. 14, 2020) ¶¶36-39. They were wrong, and they now concede it. Plaintiffs now argue that Google "conceals [the] fact" that it uses sWAA-off data for basic record-keeping by "turning off 'personalized' ads that could tip them off to Google's continued tracking." Mot. at 2:19-22. In other words, Plaintiffs have argued in this case that (1) Google fraudulently used sWAA-off data for personalization, and that (2) Google committed fraud by ***not*** using sWAA-off data for personalization. "Heads" Plaintiffs win; "tails" Google loses.

Plaintiffs' new theory is that Google misled the proposed classes because they expected that Google would stop performing basic record-keeping about the ads it serves, and indeed, stop serving ads entirely, to any user who has sWAA turned off. WAA and sWAA, in Plaintiffs' view, do not just control whether Google "saves" a user's "Web & App Activity" to that user's "Google Account" for personalization; it is also an ad blocker, which Google made available *sub silentio*. Plaintiffs' backup theory is nonsense, and it cannot be proven class-wide for three reasons.

First, Plaintiffs' only remaining claims are the tort of intrusion upon seclusion and a statutory claim for violation of CDAFA, an anti-hacking statute that, in this case, turns on privacy-related expectations. And all claims hinge on a theory that each class member withdrew consent they had given as Google Account holders for basic record-keeping by turning sWAA off. These types of claims are virtually never certified for class treatment; for a damages class, Plaintiffs cite no court that has certified one, and Google has not found one. And California courts are clear—mass torts are simply not class action material. Most relevant here, harms like emotional distress and anxiety are necessarily individualized and cannot be found to exist or not exist across the proposed 100-million person classes. Simply put, making out a case for *highly offensive conduct* and *withdrawn consent* will be all but impossible at a class-wide level, because no two Plaintiffs

were exposed to the same collection of data, and therefore no two Plaintiffs suffered the same "harm." Indeed, the named Plaintiffs themselves all testified that the supposedly offensive intrusion of their privacy has not changed their lives one iota; they still use their phones, they still use the same apps, and they do so out of convenience and preference.

Second, even if Plaintiffs could show the bare fact of harm class-wide, it is not possible to measure the class-wide harm for reasons repeatedly explored by this Court, the Ninth Circuit, and California courts. Further, Plaintiffs' damages models are patently inadmissible for a host of reasons, as demonstrated by Google's accompanying motion to strike those models.

Third, even if Plaintiffs could show harm and measure it class-wide, Google's express and implied consent defenses cannot be resolved class-wide. Plaintiffs' Motion glosses over the 1.5 million apps that were *required* to and did disclose their use of Google Analytics, albeit in myriad ways as varied as the apps themselves. Each class member, according to Plaintiffs, will have interacted with dozens of these disclosures, before and after they turned sWAA off. And Google itself disclosed what it meant when it said that the WAA and sWAA buttons affected whether data would be "saved to your Google Account"—defined terms that meant Google could still perform basic, anonymized record-keeping without contravening the sWAA control. Plaintiffs confusingly argue that the disclosures were ambiguous but that the class was confused by them in a uniform manner. But "uniform confusion" is an oxymoron; no class can be sustained on such a theory.

Plaintiffs have failed to demonstrate that their theory of the case can be proven class-wide, either for damages or for an injunctive relief class. Strong evidence presented by Google here tends to show the opposite.

II. FACTUAL BACKGROUND

A. Google never personally identifies sWAA-off Analytics or Ads data.

GA4F is used by mobile app developers "for insight on app usage and user engagement." *See* Ex. 1; *see generally* Ex. 2 (Google's Responses to Interrogatory No. 1), at 4–31; Ex. 3; & Dkt. 315-10 ("Hochman Rpt."), n.10.[1] App developers can measure various "events," or specific types

[1] References to Ex. _ draw from the Santacana Declaration filed herewith. References to Pl's Ex. _ draw from the exhibits to the Mao Declaration filed with Plaintiffs' Motion.

of user interactions within their apps. Hochman Rpt. ¶¶89–91; Ex. 2, at 4:20–5:21. Default events include the first app opening, or when a user opens a certain page of the app. Hochman Rpt., n.84; Ex. 2 at 4:20–5:21; *see also* Ex. 4. Google accepts bundles of event data from app developers' apps as a service provider and stores and analyzes them for developers regardless of a user's sWAA setting. Ex. 2, at 10:15–11:5.

App developers implement GA4F in myriad ways, but must always comply with Google's terms of use. Ex. 5 (Ganem Tr.) at 44:2–5. *See also* Ex. 6, Rebuttal Expert Report of John R. Black, Ph.D. ("Black Rpt."), ¶52, n.46 & ¶¶153–54. Developers can create custom events to supplement the default ones, Hochman Rpt., n.84 (citing "Log Events" Firebase, Google), and "user properties," which can include demographic information if the app developer sets that information for collection. Ex. 6, Black Rpt.,¶74 (citing "[GA4] User properties," Analytics Help). For example, in the data Google produced to Plaintiffs collected from their devices, 49% of over 100,000 events had no age information, 49% had no gender information, and 59% had no information about the user's interests, while the remainder had some variables set by developers. *Id.*.

If the user's sWAA toggle—the toggle that applies to data from third-party apps—is set to "off," these data are used by Google ***solely*** for the benefit of the app developer who generated the data, so they can better understand their own interactions with their own users and the success of their own advertising. Ex. 2, at 11:7-14:2. Google ***never*** tried to identify sWAA-off users, and sWAA-off data is treated by Google as "pseudonymous," just as an author may choose a pseudonym under which to write a series of novels (albeit with a random string of alphanumeric characters, not a catchy penname). *Id.*; *see also* Ex. 5 at 44:2-19. Google logs the relevant data alongside a device ID like ADID on Android or IDFA on iOS, or with other identifiers; these "pseudonymous" identifiers are ***never cross-pollinated*** with the identity of the Google Account that was using the device. Ex. 2, at 12:13-23, 13:24-14:2. Google also takes various steps to ensure nobody else can re-unify these pseudonyms to a user's identity. *Id.* at 8:7, 13:24-14:2, 15:15-23, 23:15-25:6, 27:22-28:2; Ex. 7 (Appendix X4 to Black Rpt.) & Ex. 8 (Exh. 20 to App'x, X4). To save *any* third-party activity data to a user's Google account, Google first ensures sWAA is set to "on." Ex. 2, 23-26.

Plaintiffs concede all of this; in fact, their expert acknowledged that Google "has the best intentions here" to keep pseudonymous and identifiable data separate; but, he complained, "maybe Google is nice today but they become evil in the future" and stops keeping data separate for a government or for profit. Ex. 9 (Hochman Deposition Tr.), at 364:18-365:5. He also noted that apps can violate Google's policies and send identifiable information, and he designed a test app that sent Google e-mail addresses to prove his point. *Id.* at 160:15-20. (Q: "Had you not customized your test app to send e-mail addresses, those e-mail addresses would not have been sent to Google, right?" A: "Correct. That's not a default behavior."); *see also* Ex. 6-A (App'x X2 to Black Rpt.), at 34-52. Plaintiffs do not claim that Google ever did anything with those e-mail addresses; nor could they, as "[n]othing about GA4F's design invites this or deems it permissible, and GA4F 'out of the box' does not join email addresses or other PII to any pseudonymous identifier." Ex. 6 (Black Rpt.), at 33 n.101.

B. Plaintiffs concede that Google does not personalize advertising with sWAA-off data; pivoting, they now complain about basic record-keeping.

For years, Plaintiffs made sensational allegations that Google saves sWAA-off data to marketing profiles and uses the profiles to personalize advertising: Plaintiffs claimed that Google "includes in its user profiles" data "secretly transmitted to Google" by "tracking and advertising code," *i.e.* GA4F; that by "including this data in its user profiles, Google increases the user profiles' value" and "allows Google to more effectively target advertisements to these users"; and that "this [sWAA-off] data is combined by Google into a user profile with all the other detailed, user-specific data Google collects on individuals and their devices," which "Google then uses [] to help generate billions of dollars in advertising revenues." 4th Am. Compl., Dkt. 289 1 ¶¶37-39,141-143, 146.

Plaintiffs and their experts now concede these allegations were false. Ex. 9 at 194:17-195:2; Ex. 11 at 79:15-18, 81:22-9; Mot. at 2:19-22 (arguing paradoxically that Google *conceals* its basic record-keeping activity with sWAA-off data "*by [] turning off* 'personalized' ads that could tip them off to Google's continued tracking"). **Google does not save sWAA-off data to any Google user's marketing profile, and does not use sWAA-off data for personalized advertising, either in connection with a user's true identity *or* in connection with a user's pseudonymous identity.**

See Ex. 2, Second Supp. Resp., at 7:11-15 (served Jun. 8, 2021); *id.* at 22-26; Ex. 15 at 78:2-7. Plaintiffs have known this since Google served a verified interrogatory response over two years ago. *See* Ex. 2, Second Supp. Resp., at 7:11-15 (served Jun. 8, 2021). Yet, Plaintiffs persisted. *See* 3d Am. Compl. Dkt. 138, ¶10, 123-131. Even at the close of discovery, Plaintiffs proposed re-asserting these false allegations. Order re: 4th Am. Compl., Dkt. 257 (Oct. 28, 2022).

Now, in their Motion for Class Certification, Plaintiffs pivot. Their new theory of the case is that Google contravenes its representations because, even when a user's sWAA is turned off, Google will still (1) log the fact that it has served an ad alongside a pseudonymous device identifier for accounting purposes, and (2) attribute conversion events to those ad serving records. Mot. at 14:1-6. Plaintiffs' damages expert focuses on these uses of sWAA-off data, positing "[i]f Google did not collect and save ad requests, it could not serve ads. And without data regarding both ad requests and the ads that Google served, Google would lack the records it needs to charge advertisers for its services"; further, he argues, "Google also uses this ads data to track conversions; if it lacked data regarding a user's interaction with an ad, it would be unable to determine whether that interaction is related to any later behavior." Hochman Rpt. ¶122.[2] The logging of the sWAA- off record of ad service or analytics conversion events is, in Plaintiffs' view, an indispensable link in a long chain that ends in advertisers paying for advertising.[3] Thus, Plaintiffs claim, Google should be disgorged of *all* profit made from serving *any* ads to sWAA-off users on mobile apps because, to perform the serving of the ad, Google had to keep a record that it served it. *See* Hochman Rpt., at ¶271; Ex. 11 at 129:12-18.

[2] *See also id.* ¶ 271 ("[B]ut for Google's collection of WAA-off or sWAA-off data, Google would not be able to serve advertisements to those users and then charge the advertisers because Google would lack the necessary data records to back up their advertising charges."); Ex. 11 at 113:1-3, 113:20-23 ("The advertiser would pay less to Google because Google did not – would not serve an ad in those cases. . . . They would pay them less because those ads that are currently being shown to sWAA-off users would not be shown to sWAA-off users."); *id.* at 137:2-138:14 ("My understanding is, based on input given to me, is that Google would not be able to serve an ad in those situations. Whether or not you want to call it an ad blocker, I've never called it that, but Google would not be able to serve an ad in those situations.").

[3] Plaintiffs also complain that Google uses the sWAA-off data to improve Google's products and services, (Motion p.3), and engage in fraud and spam detection, (Ex. 9 at 205:7-14, 206:19-207:3), but they do not assign these uses any value in their damages models.

At a technical level, the practice Plaintiffs complain of is the use of sWAA-off records by Google to perform "attribution" for advertisers. *See* Hochman Rpt., ¶¶279-296 (describing generally "Attribution/Conversion Tracking"); *see generally* Wikipiedia - "Attribution (marketing)"; "About Attribution" Help Center Page. Attribution can be performed in a number of ways. The specific technique Plaintiffs complain of works as follows:

1. **At Time 1**, an ad for the New York Times (NYT) app appears in the Nike app, which uses the Google Mobile Ads SDK (AdMob) to serve ads. An unidentified user clicks on it, causing the SDK to **log that the user's pseudonymous ID clicked on that ad**.

2. Then, the user installs and opens the advertised NYT app. The NYT app uses the Firebase SDK and GA4F. As a result, **at Time 2**, the NYT app uses GA4F to **log that the user's pseudonymous ID triggered the "first_open" analytics event**.

3. Google's ad system connects the dots on the back end: the same pseudonymous ID that clicked on the ad at Time 1 triggered the "first_open" event at Time 2. Google reports to the app developer/advertiser that **a conversion has occurred**, and aggregates them.

Measuring conversions varies from app to app because app developers can choose to rely on Google's default conversion events, like "first_open," or they can create their own custom conversion events, such as "open_screen_x" where "x" is a particular screen the developer wants to drive traffic to. Hochman Rpt., at 94 n.84. Plaintiffs have never offered any explanation for how this activity harms users. At all times, the activity is anonymized.

The conversion and ads logs in question are streamlined to contain just the critical pieces of information—which device triggered the event, the name of the event, which app sent Google the information, and other similar pieces of information. Ex. 6 (Black Rpt.), at 35. So, for example, while a conversion event could be called "in_app_purchase," and it could contain pseudonymous information about *what* the device purchased, for Google's attribution purposes, it is just the fact that the event occurred that is logged and later used to connect an ad click at Time 1 with a purchase at Time 2. *Id.* at 35; Hochman Report, ¶122-123.

This simple accounting is the sum and substance of Plaintiffs' case now.

C. Google gave class members comprehensive disclosure in various contexts at various times during the class period as it revised its Privacy Policy over time.

Google discloses its uses of analytics and ads data in many contexts. First, in its Privacy Policy ("PP"), Google explained throughout the class period that Google uses "cookies or similar

technologies to identify your browser or device" and to "collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites," including "Google Analytics." App'x A at 4-5. Further, the PP explained that analytics helps app owners "analyze the traffic to their [] apps" and "[w]hen used in conjunction with our advertising services . . . Google Analytics information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites." *Id.* at 5.

Plaintiffs complain about the representation that turning WAA on would enable Google to "save" a user's activity data "to your Google Account" (The sWAA control can only be enabled if WAA is also enabled.). But throughout the class period, in the PP, Google explained the difference between information "associated with your Google Account" as opposed to "non-personal information." First, the PP explained that "[i]nformation we collect when you are signed in to Google, in addition to information we obtain about you from partners, may be associated with your Google Account. **When information is associated with your Google Account, we treat it as personal information"** which can be controlled as discussed in the "Transparency and choice section of this policy [discussing WAA control]." *Id.* at 5; *see also id.* at 6-7, 11 ("Depending on your account settings, your activity on other sites and apps may be **associated with your personal information**" and Google "may share non-personally identifiable information publicly and with our partners."). Google's "How Ads Work" page, part of its Privacy Portal, also explained: "We give advertisers data about their ads' performance, but we do so without revealing any of your personal information." *Id.* at 29. Throughout the class period, the "Advertising" section of the PP explained that "[s]ometimes Google links the identifier used for advertising on mobile applications to an advertising cookie on the same device in order to coordinate ads across your mobile apps and mobile browser. . . . This also helps us improve the reports we give to our advertisers on the effectiveness of their campaigns." *Id.* at 49.

Throughout the class period, the PP directed users to a "Key Terms" section if there were phrases they did not understand: "if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first." App'x A at 1. Google defined throughout

the class period the phrases "Google Account," "personal information," and "non-personally identifiable information." *Id.* at 52. "**Google Account**" was defined as the Account a user signs up for by "providing us with some personal information" which can be used "to authenticate you when you access Google services; "**personal information**" was defined as information "which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google, **such as information we associate with your Google account**"; and "**non-personally identifiable information**" was defined as "information that is recorded about users so that it no longer reflects or references an individually identifiable user." *Id*. Further, since at least July 18, 2016, in a section linked from the Policy called "How Google uses data when you use our partners' sites or apps," Google explained that "apps that partner with Google can send us information such as the name of the app and an identifier that helps us to determine which ads we've served to other apps on your device. If you are signed in to your Google Account, and depending on your Account settings, **we may add that information to your Account, and treat it as personal information**. *Id.* at 54.

Throughout the class period, the PP has also disclosed that Google "may combine the information you submit **under your account** with information from other Google services." *Id.* at 6-7. Furthermore, "websites and apps" may use Google's "advertising services (like AdSense) or analytics tools (like Google Analytics)," which "share information about your activity with Google and, depending on your account settings and the products in use . . . may be **associated with your personal information**."). *Id.* at 24-25.

The PP also explained that "we [Google] regularly **report to advertisers on whether we served their ad** to a page and **whether that ad was likely to be seen**." App'x A at 23. Indeed, starting in April 2018, Google maintained a PP "Advertising" page that discussed, among other technologies, its ads technology. A corollary to the earlier "How Ads Work" page, this main tab of the Privacy Portal explained that "We store a record of the ads we serve in our logs," that "We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months)," and that "You can use Ads Settings to manage the Google ads you see and opt out of Ads Personalization," but "**[e]ven if you opt out of Ads Personalization, you may still see**

ads based on factors such as your general location derived from your IP address, your browser type, and your search terms." *Id.* at 57. Plaintiff Sal Cataldo understood that sWAA was not an ad blocker, and while he could control ads personalization, he knew he could not prevent Google from serving him ***any*** ads. Ex. 10 (Cataldo Tr. at 152:18-153:18).

Throughout the class period, the PP explained that users can "decide what types of data . . . you would like **saved with your account**." App'x A, at 7. The sWAA control similarly explained: "The data ***saved in your account*** helps give you more ***personalized*** experiences across all Google services. Choose which settings will save data ***in your Google Account***." 4AC, Dkt. 289, ¶77. Google thus repeatedly explained that users could affect the advertising Google serves via the "Ad Settings" button, ***not*** the sWAA button. For users who actually read these disclosures and engaged with the Ad Settings button, they would have understood that turning off the personalization setting would not prevent Google from serving ads, only make the ads less relevant. App'x A at 57. And Google disclosed that it would still perform its role as record-keeper for advertisers, and it would still serve ads, regardless of a user's Ad settings (and never represented that activity controls like WAA would have anything to do to the contrary). *Id*. Further, Google explained repeatedly that "saved with" or "saved in" your Google Account meant the same as "associated with" your Google Account and "combining" information with your Google Account, none of which includes Google's collection and use of non-personal information. *Id.* at 6-7, 24-25, 52, 54.

Google's Consumer Research expert Dr. Donna Hoffman concluded that "Google employs key UI design principles such as progressive disclosure to ensure that its notice and consent procedures are as clear as possible," which means disclosing information over time rather than all at once. Ex. 13 (Hoffman Rpt.) ¶¶21-22. Google limits disclosure to what is relevant for a user to know in context. "Providing information about the virtually unlimited set of features that the WAA settings do not control outside of their Google Accounts would overwhelm users and distract them from what is important to know about these specific settings." *Id.*

D. The classes received disparate, relevant disclosures from millions of apps.

Per Google's terms, apps must disclose and obtain consent to use the SDK. Ex. 14 (Google's Response to Interrogatory No. 18), at 6. Every time a user first opens a GA4F-enabled app, the user

thus receives a disclosure that the app uses an analytics SDK. *See* Ex. 6 (Black Rpt.) ¶153; *see also* Hochman Rpt. ¶260.

Each of the named Plaintiffs during the class period downloaded, at a minimum, forty apps that had implemented GA4F, each with distinct disclosures. *See* Ex. 15 (Pl's Resp. to Google's Interrogatory No. 8). Other users may interact with dozens of other disclosures— both before and after turning off sWAA. Indeed, some apps, like the RelayforReddit app, which Plaintiff Cataldo used, disclose GA4F by name, point users to Google's "partner policy," and explain that "[u]sers may opt-out of certain Firebase features through applicable device settings, such as the device advertising settings for mobile phones." Ex. 6 ¶161. Many apps, such as PicCollage, which Plaintiff Harvey downloaded, use and disclose GA4F *and* other third-party analytics providers, like "Flurry," "Facebook," "Amplitude," and "Fabric." *Id.* ¶162; *see also* Ex. 18, 203:5-10; Ex. 17 (App'x X5 to Black Rpt.) (cataloguing policies that disclose multiple analytics providers). Other apps, like "MyFitnessPal," which Plaintiff Cataldo downloaded in December 2010, don't name GA4F but seek user consent to share data with "certain companies for purposes of analytics and improvement" and disclose the categories of data collected and shared. *See* App'x C, at p. 15; *see general id.* (compiling disclosures from selection of apps downloaded by Plaintiffs).[4]

There are millions of distinct disclosures at issue that change over time, "due to the myriad ways app developers implement GA4F according to their business needs[.]" Ex. 6 (Black Rpt.) ¶153. Given 100 million class members and 1.5 million apps, there are endless combinations of who consented to what when. Some may have downloaded apps needing re-consent for each use. Some may have downloaded apps before turning sWAA off, and others only after. *See* Ex. 22 (Rebuttal Expert Report of Anindya Ghose, Ph.D.) ¶20. Dr. Hoffman concludes that providing this disclosure to users in each app "makes sense from a UI design perspective because it communicates information related to data collection pertaining to third-party apps where it is relevant to do so: in third-party app user agreements." Ex. 13 ¶22. Other class members may be like Plaintiff Harvey, who read the PicCollage privacy policy, but opined that "[r]egardless of what it said," Google

[4] Google also previously filed historic versions of disclosures for various apps used by plaintiffs. See Dkt. 64 (Dec. 17, 2020), which are attached here as Appendix B

"should have rejected the information," Ex. 16 at 198:4-10, even though the PP explained that Google would "respect the purposes described in the consent you give the site or app, rather than the legal grounds described in the Google Privacy Policy." *Rodriguez v. Google LLC*, No. 20-CV-04688-RS, 2021 WL 2026726, at *1 (N.D. Cal. May 21, 2021). Google's policy also provides that "[i]f you want to change or withdraw your consent, you should visit the site or app in question to do so." *Id*. Finally, many apps offer their users ways to "opt out of analytics" or to delete collected data." Ex., 15 at 6; Ex. 6 at 61, 63-64, 67-68.

E. None of Google's employees agreed that sWAA should disable record-keeping.

Absent competent evidence about the class, Plaintiffs rely on irrelevant, cherry-picked communications among Google employees to speculate about what class members are likely to think about the sWAA button. These documents are mischaracterized, unrelated to Google Analytics, or taken out of context. One study Plaintiffs point to, Mot. at 12 (citing Pl's Ex. 55, at -099.R), was "related to account creation in Europe," not any issue contested here. *See also* Ex. 13 ("Hoffman Rep.) at 92 (table). Likewise, Plaintiffs rely on an April 2020 slide deck that describes a study to evaluate users' understanding of WAA "retention" controls (how long data are retained when WAA is on). Mot. at 12 (discussing Pl's Ex. 42). That study surveyed nine participants for product development purposes—far from the methodologically sound studies used to carry the legal burden to certify a large class.

Next, Plaintiffs repeatedly quote from an email exchange between Chris Ruemmler and David Monsees. Mot. at 15 (citing Pl's Ex. 7 at -09); Mot. at 12 (citing Pl's Ex. 7 at 09, -10). Plaintiffs ignore Ruemmler's own testimony that he had a "misunderstanding" about WAA, that his work was in the Workspace and Gmail team, where "everything is GAIA tied," *i.e.* associated to a Google Account, and that he does not "work in WAA." Ex. 18 at 72-77. So, he had incorrectly assumed that "if it's not GAIA tied, it's not there." *Id.* Ruemmler stated that "after gaining more knowledge," he became aware of Google's "other mechanisms used to store the data at Google anonymously." *Id.*

None of these cherry-picked quotes help Plaintiffs' case that the avalanche of disclosures the class received warning them that basic advertising record-keeping would continue was

outweighed by the word "saved" in the description of WAA, especially since that word was followed by the phrase "to your Google Account," a defined term.

III. ARGUMENT

Plaintiffs bear the burden of proving by a preponderance of the evidence each of the class action requirements. *Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651, 665 (9th Cir. 2022). Rule 23(b)(3)'s predominance requirement "imposes stringent requirements for certification that in practice exclude most claims." *Am. Ex. Co. v. Italian Colors Rest.*, 570 U.S. 228, 234 (2013). To satisfy it, "plaintiffs must establish that essential elements of the cause of action . . . are capable of being established through a common body of evidence, applicable to the whole class." *Olean*, 31 F.4th at 666 (cleaned up). When such questions hinge on expert testimony, the Court's "determination…may include weighing conflicting expert testimony and resolving expert disputes." *Id.* (cleaned up). Further, "when individualized questions relate to the injury status of class members, Rule 23(b)(3) requires that the court determine whether individualized inquiries about such matters would predominate over common questions." *Id.* at 668.

Whether to certify a class is a claim-by-claim analysis. Class certification precedent in this District and in California relating to consumer class actions tends to relate to securities laws, consumer protection statutes, fraud claims, breach of contract, and other similar claims. But Google has not been able to locate a single Court that certified a damages class asserting a privacy tort claim (or CDAFA), in any circumstance remotely like the instant one, and for good reason: these types of claims are inherently personal, and the nature, extent, and frequency of injury and damage are highly individualized issues that are typically unsuitable for class treatment. *But see Opperman v. Path, Inc.*, No. 13-CV-00453-JST, 2016 WL 3844326, at *15 (N.D. Cal. July 15, 2016) (certifying single-app privacy tort class for nominal damages, but not damages).

A. Individual questions concerning the nature and extent of the alleged intrusions overwhelm common questions.

Every aspect of a privacy claim is fact-dependent, because, at bottom, privacy claims are focused on the harm done to the plaintiff. Plaintiffs cannot show that harm on a class-wide basis.

1. The liability elements of privacy claims are highly fact-dependent.

The California constitutional privacy claim and California intrusion-upon-seclusion claims are distinct, but because of "the similarity of the two tests, courts consider them together and ask (1) whether there is a reasonable expectation of privacy, and (2) whether the intrusion was highly offensive." *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1088 (N.D. Cal. 2022).

Plaintiffs' privacy tort is proven "only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation **or data source**." *Shulman v. Grp. W Prods., Inc.*, 18 Cal. 4th 200, 232 (1998) (emphasis added). The phrase "objective reasonableness" hides a multitude of complexities, however, "[u]nder well-settled law, in applying the objective test, a court may examine the surrounding circumstances which . . . to ascertain whether the person had a reasonable expectation that the communication would not be overheard or recorded." *Kight v. CashCall, Inc.*, 231 Cal. App. 4th 112, 133 (2014) (discussing customer phone call that was recorded). In a case relating to the collection of electronic data, "[w]hat a user would reasonably expect in light of [the defendant's] disclosures is a relevant question, but so is the amount of data allegedly collected . . . [a]nd, the nature of the allegedly collected data." *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1193 (N.D. Cal. 2020) (cleaned up).

The question of whether an intrusion is highly offensive is even more complex, because "determining offensiveness requires consideration of all the circumstances of the intrusion, including its degree and setting and the intruder's motives and objectives." *Shulman*, 18 Cal. 4th at 236. "[A]ll the circumstances of an intrusion, including the motives or justification of the intruder, are pertinent to the offensiveness element." *Id.* Some claims, like the one in *Heeger*, can be assessed at the pleading stage as clearly not highly offensive, or, as in *I.C. v. Zynga, Inc.*, the claim can fall so short of a privacy interest that Article III standing itself is found lacking. 600 F. Supp. 3d 1034, 1046, 149 (N.D. Cal. 2022) (holding "collection of email addresses, phone numbers, Zynga usernames, Zynga passwords, and Facebook usernames" was not "so private that their revelation would be highly offensive to a reasonable person" and since Plaintiffs did not allege "that any of their actual first or last names were exposed … suggesting that their anonymity is preserved," they suffered no Article III injury). In *Hammerling*, 615 F. Supp. 3d at 1090, Google's alleged collection of data subject to an allegedly "ambiguous" privacy policy provision could not be said to have

egregiously breached social norms, nor was "the data allegedly collected by Google [] sufficiently specific or personal, and its collection sufficiently harmful, to be highly offensive," even though the same Court held that the plaintiffs had a reasonable expectation of privacy in the same data. *Id.* at 1091. The court reasoned that "Courts in this district have held that data collection and disclosure to third parties that is 'routine commercial behavior' is not a 'highly offensive' intrusion of privacy." *Id.* at 1090. And in *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012), collection of "unique device identifier number, personal data, and geolocation information" did not rise to an egregious breach of social norms. *See also Cousin v. Sharp Healthcare*, No. 22-CV-2040-MMA (DDL), 2023 WL 4484441, at *6 (S.D. Cal. July 12, 2023) (holding same for "disclosing a user's browsing history").

The two leading California cases firmly rejected the possibility of certifying privacy harm classes. In *Kight*, the court held that "[a]lthough each plaintiff declared that he or she did not believe anyone was listening to the monitored calls with CashCall employees, the trier of fact would have to determine whether a person *under the particular circumstances and given the background and experience of each plaintiff* would have understood that the particular call was not being monitored." 231 Cal. App. 4th at 130 (emphasis in original). In that case, "CashCall persuasively argued that each plaintiff's factual circumstances must be considered, and cross-examination must be permitted, to determine whether each monitored telephone call was a confidential communication" in the context of a CIPA section 632 claim, which the court analyzed as analogous to a privacy tort. *Id.*; *see also Hataishi v. First Am. Home Buyers Prot. Corp.*, 223 Cal. App. 4th 1454, 1467–68 (2014) (holding same: "[W]hether an individual plaintiff had an objectively reasonable belief that his or her conversation with First American's Inside Sales group would not be recorded will require individualized proof of, among other things, the length of the customer-business relationship and the plaintiff's prior experiences with business communications." (cleaned up). And in *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 993 (2011), as *modified* (June 7, 2011), the court held that zip codes collected in order to send ads to the plaintiffs homes could not be highly offensive because they "found no case which imposes liability based on the defendant obtaining unwanted access to the plaintiff's private information which did not also allege that the *use* of plaintiff's

information was highly offensive," and obtaining mailing addresses to send advertising was not "an offensive or improper purpose," even if the method of collection was "questionable.".

The individualized circumstances of data collection and use are questions that make or break a privacy tort claim. So, too, as to Plaintiffs' CDAFA claim. California Penal Code § 502 provides for a private right of action *only* if the plaintiff can prove she was harmed by the alleged intrusion of her computer system. For this reason, CDAFA provides for highly individualized damages: compensatory damages defined as "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or destroyed by the access." Cal. Penal Code § 502(b)(11). Answering these questions as to a single plaintiff is difficult. Answering them as to 100 million plaintiffs all at once, in the context of billions of alleged intrusions will be impossible at a class-wide level, because no two Plaintiffs were exposed to the same collection of data.

2. Whether there was harm here is an individualized question.

Plaintiffs argue that they can identify what Google said and how its systems are designed class-wide. But while those were the critical questions in discovery *from Google*, the individualized issues here relate to discovery *Google* would need to take *from the 100 million privacy plaintiffs*. Proving Google's system design doesn't answer a central question class-wide because it does not imply that any specific person was ever exposed to any specific practice, and the bulk of the alleged conduct to which the classes were exposed would not even sustain Article III standing, much less the more demanding elements of Plaintiffs' claims.

Though courts sometimes intone the rule that individual damages inquiries cannot defeat class certification, the Ninth Circuit reverses district courts for failing to acknowledge that "common evidence" of "a uniform policy" can be "outweighed by the individual questions going to injury and damages." *Bowerman v. Field Asset Servs., Inc.*, 60 F.4th 459, 469 (9th Cir. 2023). In *Bowerman*, mini-trials exploring class members' individual memories would have been necessary to establish injury, fatally defeating class certification. *Id.*; *see also Castillo v. Bank of Am., NA*, 980 F.3d 723, 730 (9th Cir. 2020) (there cannot be certification for a class with "a great number of members who for some reason could not have been harmed by the defendant's allegedly unlawful conduct").

The bar for proving that a particular intrusion is highly offensive is extremely high, and rarely hit in cases like this. Plaintiffs originally alleged that Google was amassing sWAA-off data through its mobile SDKs so it could build marketing profiles for personalized advertising, but realized near the end of discovery they could not even prove that.[5] Plaintiffs' much-narrowed theory of the case relating to Google's servicing of analytics accounts and record-keeping for advertisers, all with *anonymous* data, raises significant individualized questions.

The classes Plaintiffs propose include all Google users who used apps with the GA for Firebase and/or Mobile Ads SDKs, on the theory that all of them suffered injury. But it's apparent that this cannot be. The vast majority of class members were exposed to run-of-the-mill record-keeping using unique identifiers that were not tied to any person's identity or used by Google for any purpose other than to perform accounting for the apps that generated the data or advertising in the first place. Indeed, this Court, in evaluating Plaintiffs' CIPA section 632 claim, an analog for their common law privacy tort, expressly held that they had failed to allege the data they exchanged with apps were even "confidential." Order, Dkt. 109 at 13. Since then, Plaintiffs' case has only gotten worse, not better; in the instant motion, Plaintiffs make no attempt to establish that any of the data in question is sensitive, confidential, or even meaningful to users.

Plaintiffs do not explain how they intend to prove using common evidence, in the face of this precedent, that Google's conduct was highly offensive (intrusion upon seclusion) and harmful (CDAFA) to every class member. Plaintiffs instead repeatedly assert, in circular fashion, that if their reading of the sWAA disclosures is correct, Google's upsetting its own representation is *per se* offensive and harmful, and equally so class-wide. But Plaintiffs cite no decision that so holds.

As for any app violating Google's policies, such non-uniform violations could only serve to undermine predominance further, not establish it. Yet it is just those types of atypical incidents that Plaintiffs would need to prove to be able to surmount the otherwise plainly non-actionable routine commercial behavior on which Plaintiffs reset their case, because the system as designed does not by itself rise to the level of an actionable privacy violation or CDAFA harm.

[5] Plaintiffs do say that Google *could*, if it wanted to, change the design of its systems to re-identify pseudonymous users. Of course, Google can only be liable for what it *actually does*.

3. Plaintiffs' own testimony demonstrates the predominance problem: they admitted they suffered no harm.

This Court routinely finds a predominance problem where the evidence suggests there are substantial members of the class whose conduct would not have differed even with full knowledge of an alleged misrepresentation. *See, e.g.*, *Orshan v. Apple Inc.*, No. 5:14-CV-05659-EJD, 2023 WL 3568079, at *12 (N.D. Cal. Mar. 31, 2023) ("reliance would depend on individual questions" because "a sizeable proportion of consumers who were unaware of the amount of storage space taken up by iOS 8 would still have bought the same 16 GB device if told the size of iOS 8"); *Silva v. B&G Foods, Inc.*, No. 20-CV-00137-JST, 2022 WL 4596615, at 2 (N.D. Cal. Aug. 26, 2022) (evidence buyers would have bought "0g Trans Fat[]" taco shells anyway precluded certification). Here, each one of the named Plaintiffs fatally undermined the claim of harm because each testified they had not changed their behavior phones after learning "the truth" about sWAA. *See* Ex. 19 (Knittel Rpt.) ¶¶59-68.

Plaintiff Harvey admitted that, after finding out about the alleged wrongs in this suit, she didn't delete any apps, didn't investigate those that use GA4F, won't delete her Google Account, won't switch to iOS, and won't delete any apps (unless she no longer wants to use them). Ex.16 at 244-253. When asked if she changed how much she used her Android phone since suing, Ms. Harvey said: "Why wouldn't I use my phone that I absolutely love?" *Id.* at 251:17-252:3. **Plaintiff Cataldo** similarly hasn't stopped using apps because of the alleged privacy violations. He feels only "some hesitation" and is just "more careful" on his phone, in contrast with when he used to "just pick up [his] phone and use it[.]" Ex. 10 at 187:17-24, 188:4-12, 42:19-43:25, 44:5-13. **Plaintiff Santiago** willingly engaged with the very apps he alleges violated his privacy because he liked them. Ex. 25 at 119:7-21, 162:11-20, 176:15-178:12, 180:1-11. Santiago testified, for example, that he kept using MapMyRide even after learning of Google's alleged data collection through it. His reason: "It's a great app for tracking my bike rides." He "tried other bike riding-tracking apps," but "none" did "as good a job." *Id*. at 179:14-180:11. Finally, **Plaintiff Rodriguez** admitted he did not

change his behavior, and instead willingly submitted to the alleged privacy violations.[6] Ex. 20 at 83:16-84:1, 311:8-313:9, 327:2-15, 329:11-330:6. He testified he never withdrew consent for third-party apps to collect and share his data with Google because "it doesn't matter." *Id.* at 349:5-10.

Each Plaintiff made choices, with full knowledge of "the truth," by evaluating how much they liked each app and how much they felt they needed it. Google could bring a righteous motion for summary judgment against each of them, and if denied, strong defenses at trial on this basis. But class certification will deprive Google of that opportunity as to the almost 100 million other plaintiffs who make up the proposed classes. Indeed, if, as Plaintiffs would have the Court believe, these four named plaintiffs are typical of the entire class, then a large percentage of class members would likely testify similarly on these questions.

B. Individualized inquiries for measuring harm also preclude class certification.

Class action plaintiffs must "establish that 'there is a method, common across the class, for arriving at individual damages'"; this is essential "to survive the predominance inquiry." *In re Apple iPhone Antitrust Litig.*, 2022 WL 1284104, at *16 ; *see also Bowerman*, 60 F.4th at 468–69. This is typically not practical in mass tort cases like this one. Indeed, the California Judge's Benchbook says outright that "[m]ass tort actions are not generally appropriate for class action treatment because of the number of individual factual issues concerning liability, causation, and damages." Cal. Judges Benchbook, Civ. Proc. Before Trial § 11.31. It continues: "Class certification is generally inappropriate when … The existence, type, and extent of damage varies for each class member…. and "Each class member must individually establish emotional distress damages." *Id.* § 11.32. Further, "the primary damage" in a right of privacy case "is the mental distress from having

[6] Rodriguez attempted to pass this off by claiming he was instructed not to change his behavior so counsel could discover information about his usage during the pendency of the suit. That obvious canard ignores that (1) he still acknowledged a cost/benefit calculation whereby he implicitly decided the potential to win this lawsuit outweighed the alleged highly offensive intrusion into his privacy; and (2) his testimony undermines his proffered explanation, anyway. Rodriguez *created* a new Google account (his twelfth of the ones we know about) during the lawsuit because "it's easier to do a Gmail" than a Yahoo account. Ex. 20, 312:18-20. [redacted]

been exposed to public view."[7] *Time, Inc. v. Hill*, 385 U.S. 374 384 n.9 (1967) (as quoted in CACI 1820 (2023)). Likewise, CDAFA only provides for compensatory damages defined as "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." Cal. Penal Code § 502. These types of damages are inherently personal in nature. Measuring this kind of harm, even for a single plaintiff, is notoriously difficult.[8]

Here, even if Plaintiffs could establish a bare, class-wide injury using common evidence, the inquiry cannot end there. Plaintiffs would need to have shown that something about the data collection in question went beyond routine commercial behavior, beyond even unsavory behavior, and crossed into highly-offensive-and-harmful territory. Take Plaintiffs' preferred case citation as an example. In *Opperman v. Path, Inc.*, No. 13-CV-00453-JST, 2016 WL 3844326, at *14 (N.D. Cal. July 15, 2016), the plaintiffs put forward a damages model calculated using a conjoint analysis purporting to value the allegedly ill-gotten data (there, users' contact books). Judge Tigar held that, even with the conjoint analysis, "[t]he chief problem with this analysis is that because consumers do not have identical preferences, each class member will place a very different value on the protection of — or misappropriation of — their contacts."

Here, Plaintiffs' damages theory is wholly divorced from the harms in question. For the reasons discussed in Google's accompanying motion to strike Lasinski's damages models, each of Plaintiffs' models are inadmissible, too.

---

[7] The "gist of a cause of action in a privacy case is . . . injury to the feelings without regard to any effect which the publication may have" on economic interests because the "right of privacy concerns one's own peace of mind," so "the injury is mental and subjective," as opposed to, say, the right of publicity. *Selleck v. Globe Int'l, Inc.*, 166 Cal. App. 3d 1123, 1135 (1985) (as quoted in CACI 1820 (2023)); *see also* CACI 1820 (2023) (listing damages as "Mental suffering/anxiety/humiliation/emotional distress," and special damages); BAJI 7.26 (listing "harm to the plaintiff's interest in privacy," "mental or emotional distress" and "Special damages caused by the invasion," *i.e.*, "economic losses which the plaintiff has sustained to date . . . in respect to property, business, trade, profession, or occupation"); Rest. 2d of Torts § 652H (as adopted by California courts; listing same elements).

[8] Indeed, privacy statutes with statutory damages exist in part because of the acknowledgment that measuring privacy harm is otherwise difficult to do. *See Campbell v. Facebook Inc*, 315 F.R.D. 250, 268 (N.D. Cal. 2016) ("the same difficulty that led to the creation of statutory damages also prevents plaintiffs from establishing a class-wide method of awarding damages based on Facebook's profits").

C. Individual questions concerning consent overwhelm common questions.

Google asserts defenses of express and implied consent. Plaintiffs place great emphasis on this Court's previous holding that a reasonable user may have understood that Google would not target advertising using sWAA-off data at the pleading stage. Mot. at 5 (citing Dkt. 109 at 7, 10, 16; Mot. at 11 (citing Dkt. 109 at 13). But Plaintiffs can no longer hide behind the pleading standard, and so they have conceded that their allegation was always wrong and pivoted to their theory that sWAA should have served as an ad blocker. Far from ruling that the consent question was closed, this Court was deciding whether individual named Plaintiffs stated a claim that did not by itself reveal an absolute consent defense.

1. Plaintiffs' theory relies on "uniform confusion" about sWAA.

Plaintiffs assert that their interpretation that the sWAA button serves as an ad blocker is unambiguous and may be applied to the entire class. There are several problems with this.

First, Plaintiffs' case hinges on a reading of the WAA disclosures that renders them *ambiguous*, because the unambiguous meaning of the Privacy Policy and WAA disclosure does not support their case—when WAA was turned "off," Google indeed did not save activity data to a user's Google Account, just as Google disclosed. Plaintiffs argue that Google's disclosures surrounding sWAA created confusion as to the types of data it covered and which aspects of Google's business would be disabled by turning sWAA off. *See* Mot. 12, 15, 16 (citing to internal documents at Google for proposition that users and employees were confused by function of sWAA toggle); Hochman Rpt. ¶389 (citing an internal 2017 Google study where 8/10 participants did not understand sWAA text). That is incompatible with class-wide treatment, because it necessarily concedes ambiguity in interpretation of the sWAA language, which in turn requires extrinsic evidence to resolve. *Pac. Gas & Elec. Co. v. G. W. Thomas Drayage & Rigging Co.*, 69 Cal. 2d 33, 40, (1968); *In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2014 WL 1102660, at *18 (N.D. Cal. Mar. 18, 2014). That extrinsic evidence necessarily includes the user's other experiences with Google, their exposure to other disclosures from third-party app developers, and their own personal experience with technology. *See Hart v. TWC Prod. & Tech. LLC*, No. 20-CV-03842-JST, 2023 WL 3568078, at *10 (N.D. Cal. Mar. 30, 2023) ("[C]ourts in this district have found that users

of applications implied consent through their conduct when they continued to use the applications despite exposure to materials that disclosed the challenged practices."). For example, in *Hart*, the court denied class certification because individualized inquiries required the court to evaluate "whether individual users understood…the permission prompts" in the app to allow defendant to use "the location data it collected for advertising purposes in addition to strictly weather-related purposes." *Id*. at *10. And in *Brown v. Google, LLC*, a case relating to Google's continuing servicing of Google Analytics on websites that incorporate it even if the user has enabled a "private browsing mode," Judge Gonzalez Rogers held that individualized implied consent issues overwhelmed common ones, so no damages class could be certified. *See* Case No. 4:20-cv-03664-YGR, 2022 WL 17961497, at *18 (N.D. Cal. Dec. 12, 2022).

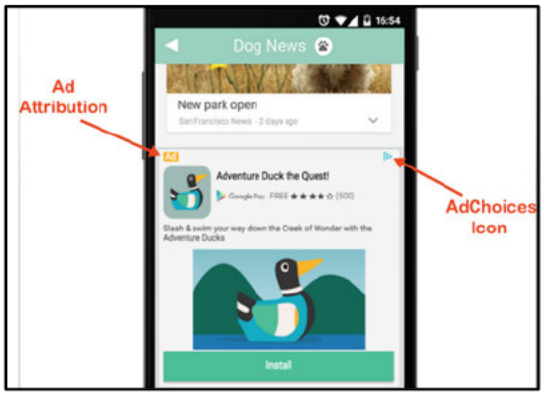
Indeed, Plaintiffs' own technical expert bent over backwards to opine that the sWAA control was misleading by inventing his own definition of "Google Account" that was at clear odds with the definition in Google's Privacy Policy, and burying it in a footnote of his report.[9] When confronted with this, he admitted his definition differed from Google's and that his opinions were all premised on his bespoke (and wrong) definition.[10]

Second, Plaintiffs' strained interpretation of the sWAA toggle could never be unambiguous because it makes no sense. Most of the class was likely well aware that sWAA would not serve as an ad blocker ***because they turned sWAA off and Google kept serving them ads***. Every member of the class who was served an ad by Google had the obvious and clear opportunity to understand that the ad was served by Google. And if it wasn't evident on its face, each class member could click on the ubiquitous blue triangle in the corner of the ad—the same symbol users are accustomed to seeing on the web—to learn that they were served that ad by Google, and to quickly change their settings

[9] Hochmans' report used the term "Google Account" at least forty times before, on page 65, he defined it in footnote 104: "By 'Google Account,' with a capital 'A,' I am referring collectively to the trove of data that Google collects and saves regarding a user, **including data that Google characterizes as 'pseudonymous**[.]'"

[10] Hochman conceded that he's "pretty sure [he] may have crossed the wires at some point" and mixed up where he "may have said Google Account when [he] really meant Google log-in[.]" Ex. 9 at 38:6-14. Hochman acknowledged that Google defines the terms differently, but defended himself on the grounds that "[w]hat they think it means may be different than what I think it means." *Id.* 39:14-18.

to see fewer ads from that advertiser, to turn personalization on or off, and other similar choices. Google's policies require the inclusion of the blue triangle "Ad badge and AdChoices icon" on Google ads.



Indeed, Plaintiff Cataldo understood Google's disclosures perfectly. He testified that, in his view, the GAP button controls ad personalization, while the sWAA button controls which data could be used for that personalization. He admitted that with GAP on, "I would say the ad settings are allowing the information I've shared to Google to potentially be used to personalize my ads saying, Do you want us to use information that we have to personalize your ads?" Ex. 10 at 152: 21-153:1. But with the sWAA controls on, Google cannot collect new sWAA data to use in personalizing ads: "So my expectation is, if I've told Google don't take certain information using the WAA setting, I don't have to have the ad setting off." Ex. 10 at 153:3-8. Cataldo correctly understood exactly how both controls were designed to function. *See* Ex. 5 at 44:2-19.

Third, each member of the class *did have a way to prevent conversion attribution* throughout the class period, and many used it. Google and Apple both offered a device-level control for this purpose; on Android, it is called "OOOAP" or "Opt out of Ad Personalization"; on iOS, it was called "Limit Ad Tracking (LAT)," and is now called "App Tracking Transparency." Starting with iOS 14.5 in April 2021, iOS forced *all* users to opt-***in*** to ad tracking affirmatively, yet Plaintiffs include users who, over the last two years, opted in to ad tracking, even though they obviously consented, as well as users who opted out, who thereby disabled Google from being able to perform the very attribution Plaintiffs claim is actionable. *See* Ex. 21 (Google's Resp. to Interrogatory No. 17); Ex. 5, at 72:4 - 72:22; Ex. 6, at 39-40. Regardless, many users were aware of, and successfully used, device controls like OOOAP, LAT, and ATT to disallow Google's logging of ad record data alongside their pseudonymous identifiers.

Finally, for accounts created before 2016, sWAA was off by default. Hochman Rpt. ¶¶54-55. For those accounts, it's not clear that any user ever made a decision to turn it off at all. Plaintiffs

have presented no method of separating those users from the rest of the class, but Plaintiffs' technical expert acknowledges that "WAA and sWAA states are 'sticky,' meaning it is unlikely for users to frequently change the setting state." *Id*. ¶51.

2. Disparate third-party disclosures undermine predominance.

As described above, each class member was subjected to dozens, perhaps hundreds, of disclosures from apps informing them that their activity data on third party apps was being collected. Ex. 14, at 6; Ex. 6 at 65; *see also* Ex. 20 ¶20 (users may have understood third party disclosures as governing app activity data instead of Google's policies). Ultimately, the fact-finder will have to evaluate which of the various sources of disclosure each individual saw. *In re Google Inc.Gmail Litig..*, 2014 WL 1102660, at *18 ("Some Class members likely viewed some of these Google and non-Google disclosures, but others likely did not. A fact-finder, in determining whether Class members impliedly consented, would have to evaluate to which of the various sources each individual user had been exposed and whether each individual 'knew about and consented to the interception' based on the sources to which she was exposed"); *Hart*, 2023 WL 3568078, at *11 ("The factual questions of whether users viewed any of these materials prior to or during their use of the App and whether users who viewed these materials and continued to use the App thereafter necessitate individualized factual inquiries" regarding "reasonable expectation of privacy.").

Here, the fact-finder will have to conduct a consent inquiry for each user and each of the innumerable permutations of apps the user has downloaded. For example, even if it were plausible that Google's disclosures could be read to say that the sWAA button served as an ad blocker, the trier of fact would have to consider the app's disclosures themselves in evaluating consent. *Thomas Drayage*, 69 Cal. 2d at 40. The trier of fact would also have to evaluate whether an app developer offered their end users with ways to "opt out of analytics usage" or otherwise "delete data the developer has collected from that user's device and sent to Google." Ex. 28 at 6; Ex. 6 at 63-64, 67-68. The fact-finder would then have to conduct that analysis for each app the user had. Each app's disclosures could have also changed over time, so the analysis could vary depending on when the user downloaded an app. And Google should have the right to challenge each class member's claim

that they ignored each and every one of those disclosures because of an idiosyncratic reading of the sWAA button.

And, even if it were crystal clear that sWAA served as an ad blocker (it is not), consent would still require individualized inquiries to evaluate whether the user turned off the sWAA button before or after agreeing to the privacy policy and terms of service for each app. Under California law, where there are multiple written instruments dealing with the same subject matter, "the contracts must be interpreted together and the latter contract prevails to the extent they are inconsistent." *Suski v. Coinbase, Inc.*, 55 F.4th 1227, 1230–31 (9th Cir. 2022) (citing *Capili v. Finish Line, Inc.*, 116 F. Supp. 3d 1000, 1004 n.1 (N.D. Cal 2015), *aff'd*, 699 F. App'x 620 (9th Cir. 2017) (quoting 17A C.J.S. Contracts § 574)); *see also Williams v. Atria Las Posas*, 24 Cal. App. 5th 1048, 1052 (2018). Here, many if not most of the class members encountered the user agreements established by the GA4F-enabled mobile apps *after* the class member turned off the sWAA toggle. In some cases, a user will have turned sWAA off and then agreed to dozens of privacy policies disclosing the use of a Google ads or analytics SDK. Those latter agreements should prevail over the switching off of the sWAA toggle.

D. No injunctive relief class should be certified.

Plaintiffs' "primary intent in this litigation is to recover damages for past [conduct]," and therefore certification of an injunctive class is not appropriate here. *In re Flash Memory Antitrust Litig.*, 2010 WL 2332081, at *7 (N.D. Cal. June 9, 2010); *see also Zinser v. Accufix Rsch. Inst.*, *Inc.*, 253 F.3d 1180, 1195 (9th Cir. 2001). Furthermore, the basic requirement for an injunctive relief class is not met here, because Google has not "acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole[.]" *Sidibe v. Sutter Health*, 333 F.R.D. 463, 498–99 (N.D. Cal. 2019). "The key to the (b)(2) class is 'the indivisible nature of the injunctive or declaratory remedy warranted—the notion that the conduct is such that it can be enjoined or declared unlawful only as to all of the class members or as to none of them.'" *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 360 (2011). That is, the defendant must have "acted in a consistent manner toward members of the

class so that the [defendant]'s actions may be viewed as part of a pattern of activity, or has established or acted pursuant to a regulatory scheme common to all class members." Wright & Miller, 7AA Fed. Prac. & Proc. Civ. § 1775 (3d ed.); *see also Nevarez v. Forty Niners Football Co.*, 326 F.R.D. 562, 590 (N.D. Cal. 2018). Class certification for injunctive relief is appropriate where "uniform relief from a practice [is] applicable to all" class members. *See Vietnam Veterans of Am. v. C.I.A.*, 288 F.R.D. 192, 217 (N.D. Cal. 2012).

Here, Google did not act or refuse to act in a manner applicable to all class members. None of Plaintiffs' four items of requested injunctive relief, Mot. at 25, addresses any "common policy" by Google. The data collection here depends on numerous factors such as other user controls, app developer choices, and user engagement with apps. Requiring Google to, *e.g.*, delete already collected data and any products built using the data would be grossly overbroad. And no trial on an injunctive relief claim would result in a judgment, because Google's individualized defenses would still apply as to each class member.

Further, Plaintiffs' request is infeasible, goes far beyond the alleged harm, and would detrimentally affect Google users outside the class. To satisfy this request, Google would have to identify each and every class member and associate it with pseudonymous sWAA-off data in order to delete their data. This would require Google to contravene its policies against joining pseudonymous data with user accounts, and its policies forbidding fingerprinting, and perform the exact invasion of privacy Google has steadfastly refused to commit even as it stands accused of doing just that. There is simply no reason for certification of an injunctive relief class here. Indeed, for their California law claims, Plaintiffs don't need a class action to secure injunctive relief that benefits the public.

IV. CONCLUSION

For the foregoing reasons, Defendant respectfully requests that the Court deny Plaintiffs' Motion for Class Certification.

Dated: August 24, 2023

WILLKIE FARR & GALLAGHER LLP

By: */s/ Eduardo E. Santacana*

Benedict Y. Hur
Simona Agnolucci
Eduardo E. Santacana
Noorjahan Rahman
Argemira Flórez
Harris Mateen

Attorneys for Defendant
Google LLC